PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : H04L 9/32 | A1

(11) Internationale Veröffentlichungsnummer: **WO 00/67422**

(43) Internationales Veröffentlichungsdatum: 9. November 2000 (09.11.00)

(21) Internationales Aktenzeichen: PCT/DE00/01086

(22) Internationales Anmeldedatum: 7. April 2000 (07.04.00)

(30) Prioritätsdaten:
199 19 909.4 30. April 1999 (30.04.99) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: WINCOR NIXDORF GMBH & CO. KG [DE/DE]; Heinz–Nixdorf–Ring 1, D–33106 Paderborn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: NOLTE, Michael [DE/DE]; Koberg Weg 2a, D–33034 Brakel (DE).

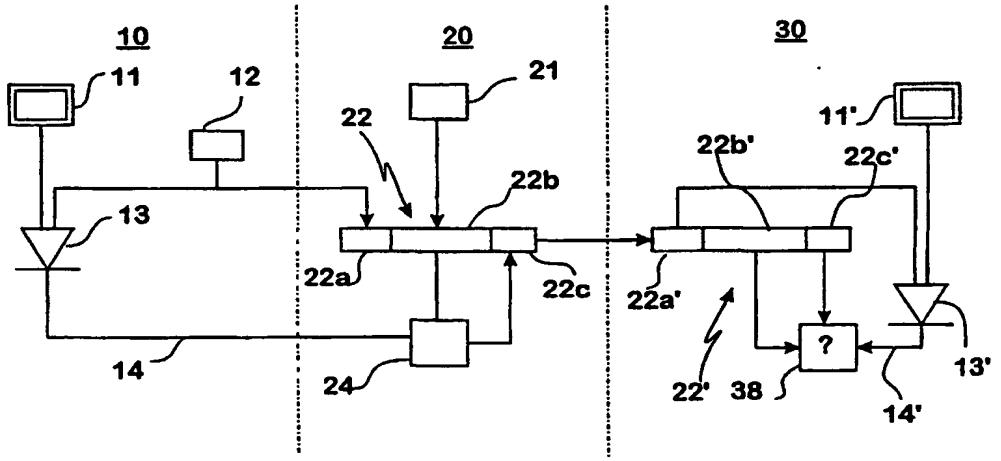
(74) Gemeinsamer Vertreter: WINCOR NIXDORF GMBH & CO. KG; Heinz–Nixdorf–Ring 1, D–33106 Paderborn (DE).

(81) Bestimmungsstaaten: NO, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: SIGNING AND SIGNATURE AUTHENTICATION OF MESSAGES

(54) Bezeichnung: SIGNIERUNG UND SIGNATURPRÜFUNG VON NACHRICHTEN



(57) Abstract

The invention relates to a method for signing a message. A control centre and the receiver have a permanent mutual master key. The control centre first provides a sequential number and, based thereupon, provides a signature key by means of a one–way function. Said number and said key are provided to the transmitter in a protected manner. The transmitter produces a signature of the message by means of the signature key and sends the signature, the sequential number and the message to the receiver. The receiver produces an authentication key by means of the one–way function, the master key and the sequential number and authenticates the signature of the message therewith.

(57) Zusammenfassung

Verfahren zur Signierung einer Nachricht, wobei eine Zentrale und der Empfänger einen permanenten gemeinsamen Hauptschlüssel haben. Die Zentrale erzeugt vorab eine Sequenzzahl und aus dieser mittels einer Einwegfunktion einen Signierschlüssel. Beides wird gesichert dem Absender bereitgestellt. Der Absender bildet mittels des Signierschlüssels eine Signatur der Nachricht und sendet sie mit Sequenzzahl und Nachricht an den Empfänger. Der Empfänger bildet mittels Einwegfunktion, Hauptschlüssel und Sequenzzahl einen Prüfschlüssel und prüft damit die Signatur der Nachricht.

Signierung und Singnaturprüfung von Nachrichten

Technisches Gebiet

Die Erfindung betrifft die Signierung und Singnaturprüfung von Nachrichten unter Verwendung geheimer Schlüssel.

Stand der Technik

Für die Fälschungssicherung von Nachrichten ist bekannt, daß mit Hilfe von symmetrischer Kryptographie eine Signatur gebildet wird, mittels derer der Empfänger mit sehr hoher Wahrscheinlichkeit prüfen kann, ob die Nachricht unverfälscht übermittelt wurde und von dem vorgegebenen Absender stammt. Voraussetzung ist jedoch, daß Absender und Empfänger über einen gemeinsamen geheimen Schlüssel verfügen, der sicher gespeichert sein muß. Ein solches Verfahren ist beispielsweise in der Patenschrift US 4,549,075 beschrieben.

Symmetrische Kryptographie, insbesondere das DES-Verfahren, wird häufig in Chipkarten eingesetzt, weil es sehr effizient programmierbar ist. Die Chipkarten weisen ferner einen Permanentspeicher auf, in dem ein Hauptschlüssel sicher geheim gespeichert ist, der auch in einer Zentrale sicher gespeichert ist.

Soll nun eine Nachricht fälschungsgesichert von einem Absender an den Empfänger, hier die Chipkarte, gesendet werden, so muß bislang der Absender die Nachricht von der Zentrale signieren lassen, da die Zentrale den geheimen Hauptschlüssel nicht dem Absender zur Verfügung stellen kann,

ohne das Gesamtsystem zu schwächen. Zudem sind Maßnahmen notwendig, damit die Nachricht bei der Übertragung von dem Absender zur Hauptstelle gegen Verfälschung und Vortäuschung eines legitimen Absenders geschützt ist.

Aufgabe der Erfindung ist es daher, ein Verfahren zur Fälschungssicherung von Nachrichten durch eine Signatur anzugeben, die von einem Absender gebildet und zu einem Empfänger gesendet werden kann, ohne daß der Absender über den geheimen Hauptschlüssel verfügt, den der Empfänger und eine Zentrale gemeinsam haben, oder die Nachricht zuvor zu der Zentrale zwecks Signaturbildung gesendet werden muß.

Darstellung der Erfindung

Die Erfindung benutzt ein Verfahren, bei dem die Zentrale Signierschlüssel vorab bildet und dem Absender bereitstellt. Der Empfänger kann, wie genauer in den Ausführungsbeispielen beschrieben wird, den Signierschlüssel nachbilden und damit die Nachricht prüfen.

Es handelt sich um ein Verfahren zur Signierung einer Nachricht, wobei eine Zentrale und der Empfänger einen permanenten gemeinsamen Hauptschlüssel haben. Die Zentrale erzeugt vorab eine Sequenzzahl und aus dieser mittels einer Einwegfunktion einen Signierschlüssel. Beides wird gesichert dem Absender bereitstellt. Der Absender bildet mittels des Signierschlüssels eine Signatur der Nachricht und sendet sie mit Sequenzzahl und Nachricht an den Empfänger. Der Empfänger bildet mittels Einwegfunktion, Hauptschlüssel und Sequenzzahl einen Prüfschlüssel und prüft damit die Signatur der Nachricht.

Weitere Merkmale und Vorteile der Erfindung ergeben sich aus der folgenden Beschreibung, welche in Verbindung mit den beigefügten Zeichnung die Erfindung an Hand eines Ausführungsbeispiels erläutert.

Kurzbeschreibung der Zeichnung

Es zeigt

Fig. 1 ein Diagramm, in dem der Datenfluß mit den beteiligten Komponenten symbolisiert ist.

Beschreibung mindestens einer Ausführungsform mindestens der Erfindung

In Fig. 1 sind die drei Teilnehmer an dem Verfahren, nämlich die Zentrale 10, der Absender 20 und der Empfänger 30, durch punktstrichlierte Linien getrennt, angedeutet.

Die Zentrale 10 enthält einen gesicherten Speicher 11 für einen geheimen Schlüssel, der ansonsten beispielsweise in einem symmetrischen kryptographischen Verschlüsslungs- oder Signierverfahren verwendet wird. Der Empfänger 30 enthält einen entsprechenden Speicher 11', der denselben Schlüssel enthält. Das Einschreiben dieses Schlüssels erfolgt beispielsweise in der Zentrale bei der Initialisierung, wenn es sich bei dem Empfänger 30 um eine Chipkarte handelt. Andernfalls sind aus der Kryptographie bekannte Schlüsselverteilungsverfahren anzuwenden. Dabei wird der Schlüssel nur einmal oder in sehr großen Zeitabständen gespeichert; für das Verfahren nach der Erfindung ist die Speicherung als permanent anzusehen.

Die Zentrale 10 enthält ferner einen Sequenzgenerator 12. Dieser liefert eine Reihe von jeweils unterschiedlichen Zahlen. Im einfachsten Fall ist dies eine fortlaufende Nummer. Besser ist jedoch die Verwendung eines bekannten Pseudo-Zufallszahlengenerators, z.B. nach der Modulo-Methode. Bei richtiger Wahl der Parameter liefern diese Pseudo-Zufallszahlen-Generatoren eine Folge von jeweils neuen Zahlen, bis der durch den Modulus bestimmte Zyklus durchlaufen ist. Auch können absteigende Nummern oder solche mit einer Schrittweite größer als Eins verwendet werden. Gleichfalls möglich ist die Verwendung von Datum und Uhrzeit als eindeutig Sequenznummer, gegebenenfalls als Zahl der Sekunden seit einem verabredeten Beginn.

Die Zentrale erzeugt also ein oder mehrere Sequenznummern 12. Aus einer solchen Sequenznummer 12 wird mittels des Hauptschlüssels durch einen Einweg-Verschlüssler 13 ein Signierschlüssel 14 gebildet. Dies geschieht am einfachsten, indem die Sequenznummer 12 mittels des Hauptschlüssels verschlüsselt wird. Hierbei wird eine kurze Sequenznummer durch weitere Daten auf die Blocklänge des Verschlüsslungsverfahrens aufgefüllt. Zwar sind hierzu binäre Nullen verwendbar; besser ist eine Funktion der Sequenznummer, z.B. deren Quadrat. Auch möglich ist ein konstanter Text, der nicht aus binären Nullen besteht und vertraulich gehalten wird. Da meist die Blockgröße in der Größenordnung der Schlüssellänge liegt, ist das Ergebnis als Schlüssel weiterverwendbar; gegebenfalls sind Bits aufzufüllen oder durch Faltung die Bitzahl zu reduzieren.

Wesentliche Eigenschaft des Einweg-Verschlüsslers ist es, daß ein Rückschluß auf den Hauptschlüssel praktisch nicht

möglich ist. Obwohl die soeben beschriebene Methode keine Einweg-Verschlüsslung ist, weil z.B. der Empfänger durch Dechiffiriern aus dem Signierschlüssel die Sequenzzahl bilden könnte, ist die "Einweg"-Funktionalität wesentlich.

Daher werden in anderen Ausführungsformen andere Einweg-Funktion verwendet, die Hauptschlüssel und Sequenznummer reproduzierbar zu einem Signierschlüssel verknüpfen, ohne daß jemand ohne den Hauptschlüssel zu einer gegebenen Sequenznummer einen gültigen Signierschlüssel bzw. umgekehrt bilden oder aus dem Signierschlüssel und der Sequenznummer den Hauptschlüssel bestimmen kann. Solche Verfahren werden allgemein als "Message Authentication Codes" (MAC) bezeichnet. Ein solcher kann insbesondere durch eine beliebige, kryptographisch sichere Einweg-Funktion auf eine Kombination von Hauptschlüssel und Sequenznummer gebildet werden. Als Kombination sind u.a. Konkatenation, Exklusiv-Oder, Multiplikation mit oder ohne Modulobildung, Addition möglich.

Die Zentrale 10 stellt also ein oder mehrere Paare von Sequenznummer 12 und daraus erzeugtem Signierschlüssel 14 bereit. Dies kann z.B. Ausdrucken auf Sicherheitspapier, durch Einspeichern in eine weitere Chipkarte oder durch sonstige gesicherte Datenübermittlung geschehen. Diese Paare werden dem Absender 20 vorab zur Verfügung gestellt und müssen von diesem gesichert und vertraulich gespeichert werden.

Der Absender 20, der eine Nachricht 21 an den Empfänger 30 senden möchte, entnimmt ein Paar von Sequenznummer 12 und Signierschlüssel 14 und bestimmt die Signatur der Nachricht 21 mittels des Signieres 24. Bevorzugt wird auch hierbei

das DES-Verfahren, z.B. nach ANSI X9.9, verwendet. Alternativ kann eine Signatur durch eine Kombination einer kryptographischen Hash-Funktion mit einem "message authentication code" erzeugt werden. Verfahren hierzu sind in der kryptographischen Literatur vielfach und ausführlich beschrieben.

Sodann bildet der Absender eine Datensatz 22, der drei Felder mit der Sequenznummer 22a, der Nachricht 22b und der Signatur 22c enthält. Der soeben verwendete Signierschlüssel 14 wird gelöscht.

Nunmehr wird der Datensatz 22 zu dem Empfänger 30 übertragen, welcher damit einen Datensatz 22' erhält, der wiederum drei Felder enthält, die als Sequenznummer 22a', Nachricht 22b' und Signatur 22c' angesehen werden. Üblicherweise wird dieser Datensatz bereits von anderen Sicherungs- oder Plausibilitäts-Mechanismen gegen Übertragungsfehler gesichert.

Der Empfänger extrahiert aus dem empfangenen Datensatz 22' die Sequenznummer 22a' und führt diese zusammen mit dem Hauptschlüssel 11' einer Einweg-Verschlüsslung 13' zu, die dieselbe wie die Einweg-Verschlüsslung 13 in der Zentrale 10 bzw. dazu funktionsgleich ist. Am Ausgang der Einweg-Funktion entsteht ein Prüfschlüssel 14'. Dieser ist, wenn die Sequenznummer korrekt übertragen wurde, gleich dem Signierschlüssel 14, den der Absender 20 verwendet hat. Der Prüfschlüssel 14' wird zusammen mit der eingetroffenen Nachricht 22b' und der eingetroffenen Signatur 22c' einem Signaturprüfer 38 zugeführt wird. Passen alle drei zueinander, erzeugt der Signaturprüfer 38 an seinem Ausgang ein Freigabesignal für die Weiterverwendung der Nachricht. Der Prüfschlüssel 14' wird, unabhängig von dem Ergebnis, mit Abschluß der Prüfung vernichtet.

In einer Weiterbildung der Erfindung führt der Empfänger eine Liste bereits benutzter Sequenzzahlen und weist Nachrichten mit bereits verwendeten Sequenzzahlen ab. Damit ist eine zusätzliche Sicherheit gegen Mißbrauch gegeben.

Da die die Sequenzzahl bevorzugt durch einen deterministischen Generator erzeugt wird, kann die Übermittlung der Sequenzzahl entfallen. Da ohnehin der gemeinsame Hauptschlüssel in gesicherter Umgebung an den Empfänger übertragen werden muß, kann zugleich der Anfangswert des Generators übertragen werden. Mit jeder empfangenen Nachricht erzeugt der Empfänger einen neuen Wert für die Sequenzzahl und bildet damit den Prüfschlüssel 14', ohne daß die Sequenzzahl mit übertragen werden muß. Um robust gegenüber Doppelübertragungen und verlorene Nachrichten zu sein, wird dann zweckmäßig auch einer der letzten und folgenden Sequenzahlen mit verwendet werden. Auch hier kann die Zentrale dem Absender mehrere Signierschlüssel 14 bereitstellen, die dann vom Absender in der vorgegebenen Reihenfolge verwendet werden sollen.

Eine mögliche Anwendung der Erfindung liegt auf dem Gebiet der Geldausgabeautomaten. Die Zentrale ist dabei die Bankenzentrale, die für die Prüfung der PIN einen Hauptschlüssel verwendet und an den Hersteller von Geldautomaten in der Zentrale personalisierte Prüfmoduln liefert. Als Absender kommt ein Hersteller oder eine lokale Bankenorgansation in Betracht, die beispielsweise einen Umrechnungskurs oder einen Rabattsatz in den Geldausgabeautmaten laden möchte; aber weder einen eigenen geheimen Schlüssel in den Geldautomaten einbrigen kann noch einen eigenen Sicherheitsmodul einbauen möchte.

Falls kein nichtflüchtiger Speicher im Empfänger vorhanden ist, kann der Empfänger auch die Sequenzzahlen von Anfang erzeugen und mit jeder die Signatur verproben. Der Verlust an Sicherheit ist dabei gering, jedoch ist keine Sicherhiet gegen Doppelbenutzung gegeben.

Patentansprüche

1. Verfahren zur Signierung einer Nachricht (22) durch einen Absender (20) und Prüfung der Signatur durch einen Empfänger, wobei eine Zentrale (10) und ein Empfänger (30) über einen geheimen gemeinsamen Hauptschlüssel (11, 11') verfügen, mit den Merkmalen:

   - Die Zentrale (10)
     * erzeugt eine Sequenzzahl (12) und
     * aus dieser unter Verwendung des Hauptschlüssels (11) mittels einer Einweg-Verschlüsslung (13) einen Signierschlüssel (14) und
     * stellt dem Absender den Signierschlüssel (14) bereit;
   - der Absender (20)
     * bildet mittels des Signierschlüssels (14) eine Signatur (22c) über die Nachricht (21, 22c) und
     * sendet an den Empfänger einen Nachrichtensatz (22), der zumindest die Nachricht (22b) und die Signatur (22c), enthält.
   - Der Empfänger (30)
     * bestimmt die Sequenzzahl (22a'),
     * bildet den mittels der Einweg-Verschlüsslung (13') und dem Hauptschlüssel (11') einen Prüfschlüssel (14') und
     * prüft damit die Signatur (22c) der Nachricht.

2. Verfahren nach Anspruch 1, wobei die Sequenzzahl (12, 22a, 22a') zusammen mit dem Signierschlüssel (14) von

der Zentrale an den Absender (20) übergeben und von diesem über den Datensatz (22, 22') an den Empfänger übergeben wird.

3. Verfahren nach Anspruch 1, wobei die Sequenzzahl (12) durch einen Generator synchron zu der Anzahl der verwendeten Signier- bzw. Prüfschlüssel in der Zentrale (10) und bei dem Empfänger erzeugt wird.

4. Verfahren nach Anspruch 1, wobei die Sequenzzahl (12) durch einen Generator synchron zu der Anzahl der verwendeten Signier- bzw. Prüfschlüssel in der Zentrale (10) und bei dem Absender erzeugt und über den Datensatz (22, 22') an den Empfänger übergeben wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Sequenzzahl durch einen Generator für Pseudo-Zufallszahlen erzeugt wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei als Einweg-Verschlüsslung die Verschlüsselung der Sequenzzahl mittels des Hauptschlüssels verwendet wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Zentrale (10) vorab mehrere Signierschlüssel (14) erzeugt und diese, ggf. gemeinsam mit den zugehörigen Sequenzzahlen (12), an den Absender (30) übermittelt.

8. Verfahren nach einem der vorhergehenden Ansprüche, wobei der Empfänger (30) eine Liste bereits verwendeter Sequenzzahlen führt und bereits verwendete Sequenzzahlen abweist.

9. Einrichtung zur Signierung einer Nachricht (22, 22'), die von einem Absender (20) an einen Empfänger (30) geschickt wird, mit den Merkmalen:

- Eine Zentrale (10) und der Empfänger (30) verfügen über einen ersten und zweiten Speicher für einen geheimen gemeinsamen Hauptschlüssel (11, 11');
- in der Zentrale (10) ist ein erster Einweg-Verschlüssler (13) an einem Eingang mit dem ersten geschützten Speicher (11), an einem anderen Eingang mit einem Generator (12) für eine Sequenzzahl verbunden,
- der Ausgang des Einweg-Verschlüsslers (13) ist über ein Transportmedium mit dem Absender (20) verbunden,
- beim Absender ist ein Signatur-Generator (24) vorgesehen, dessen Eingänge mit dem Ausgang des Einweg-Verschlüsslers und der zu signierenden Nachricht (21, 22b) verbunden sind,
- der Ausgang des Signatur-Generators (24) ist mit einer Einrichtung verbunden, die mindestens die Signatur (22c) und die Nachricht (22b) zu einem Nachrichtenblock (22) assembliert und deren Ausgang über ein Transportmedium mit dem Empfänger (30) verbunden ist,
- im Empfänger ist ein Signatur-Prüfer (22') vorgesehen, an dessen Eingänge einerseits mit der Nachricht (22b') und der Signatur (22c') des über das Transportmedium eingetroffenen Nachrichtenblocks (22'),
- andererseits mit dem Ausgang eines zweiten Einweg-Verschlüsslers (13') verbunden ist, dessen Eingänge einerseits mit dem zweiten Speicher (11') für den ge-

heimen Hauptschlüssel und mit einem Mittel zur Bereitstellung einer Sequenznummer (22a') verbunden ist.

10. Einrichtung nach Anspruch 9, wobei ein Generator die Sequenzzahl (22a') nach einem deterministischen Verfahren ein oder meherere Sequenzzahlen entsprechend der Anzahl der Prüfungen erzeugt.

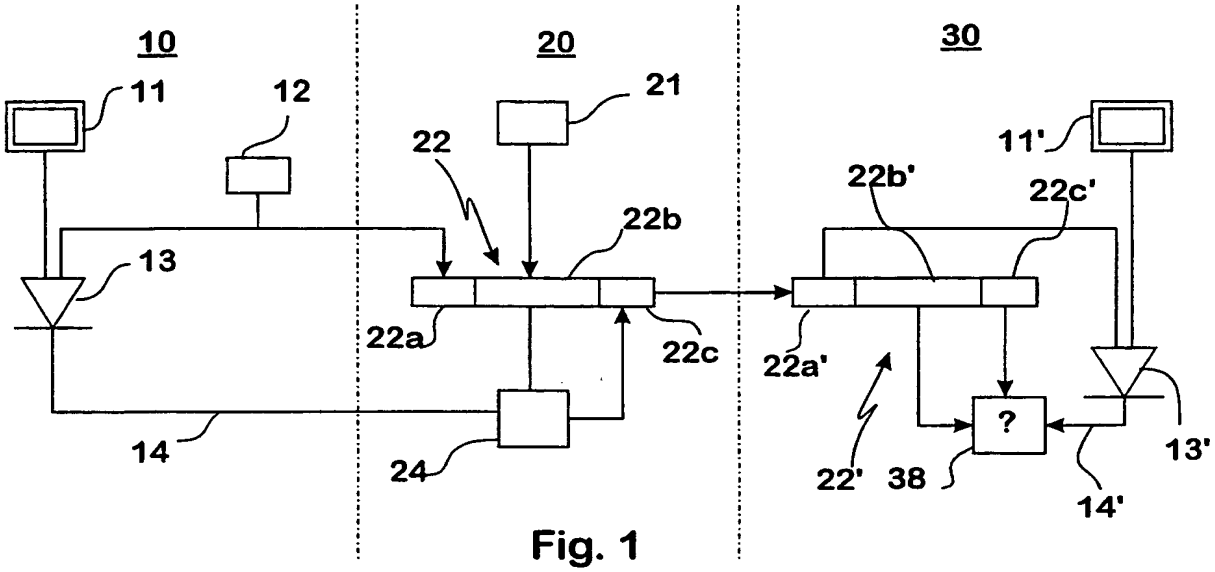


Fig. 1

INTERNATIONAL SEARCH REPORT

Inter onal Application No
PCT/DE 00/01086

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 93 21711 A (SIEMENS AG ;SIEMENS NIXDORF INF SYST (DE); HOFFMANN GERHARD (DE);) 28 October 1993 (1993-10-28) page 3, line 11 - line 27 page 4, line 22 -page 6, line 8 page 6, last paragraph	1,5,6,9
A	EP 0 077 238 A (CII HONEYWELL BULL) 20 April 1983 (1983-04-20) page 4, last paragraph -page 5, line 36 page 11, line 13 -page 15, line 10	1,9

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 August 2000	23/08/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter. nal Application No
PCT/DE 00/01086

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9321711 A	28-10-1993	DE 59305159 D	27-02-1997
		EP 0635181 A	25-01-1995
		US 5608800 A	04-03-1997
EP 0077238 A	20-04-1983	FR 2514593 A	15-04-1983
		DE 3268974 D	20-03-1986
		JP 1493553 C	20-04-1989
		JP 58075267 A	06-05-1983
		JP 61026111 B	19-06-1986
		US 4656474 A	07-04-1987

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 00/01086

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	WO 93 21711 A (SIEMENS AG ;SIEMENS NIXDORF INF SYST (DE); HOFFMANN GERHARD (DE);) 28. Oktober 1993 (1993-10-28) Seite 3, Zeile 11 - Zeile 27 Seite 4, Zeile 22 -Seite 6, Zeile 8 Seite 6, letzter Absatz	1,5,6,9
A	EP 0 077 238 A (CII HONEYWELL BULL) 20. April 1983 (1983-04-20) Seite 4, letzter Absatz -Seite 5, Zeile 36 Seite 11, Zeile 13 -Seite 15, Zeile 10	1,9

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
16. August 2000	23/08/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Inter. nales Aktenzeichen
PCT/DE 00/01086

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9321711 A	28-10-1993	DE 59305159 D	27-02-1997
		EP 0635181 A	25-01-1995
		US 5608800 A	04-03-1997
EP 0077238 A	20-04-1983	FR 2514593 A	15-04-1983
		DE 3268974 D	20-03-1986
		JP 1493553 C	20-04-1989
		JP 58075267 A	06-05-1983
		JP 61026111 B	19-06-1986
		US 4656474 A	07-04-1987